BEDC Electricity PLC
5, Akpakpava Street, Benin City, Edo State, Nigeria

Policy Area	Information		
Title of Policy	**POLICY ON THE CLASSIFICATION OF INFORMATION**		
Reference No.			
Version	1.0		
Policy Owners	All Staff of BEDC		
No. of Revision	0		
Date of Draft	4th July 2022		
Effective Date			
Approve By	*Role*	*Name*	*Signature/Date*
	MD/CEO	**Dr. Henry Ajagbawa**	
	Board of Directors		

INTRODUCTION

This document serves to outline BEDC's policy on the classification of information. Information is a set of data generated by or for, owned by, or otherwise in the possession of BEDC that is related to the company's activities. The purpose of this policy is to provide a framework for the protection of information that is created, stored, processed, or transmitted within BEDC. The classification of information is the foundation for the specification of policies, procedures, and controls necessary for the protection of confidential data. Data and information are used interchangeably in this policy.

SCOPE

This policy applies to data in any form, such as electronic, printed, audio visual, and includes live, backup, and archived data, which could be proprietary, externally acquired, or third-party sourced. It applies to all BEDC's employees including individuals working on a permanent, contract and secondment basis, as well as to contractors, Board members and third-party agents authorized to access the data.

ROLES AND RESPONSIBILITIES

This includes individuals working on a permanent, contract and secondment basis as well as contractors, Board members or those employed through an agency.

a. The Board has delegated day-to-day responsibility for policy compliance to the MD/CEO.
b. The Chiefs, Regional Heads (RH) and Heads of Departments (HODs) shall be the data owners, and they shall be responsible for data classification within their functional areas. They are directly accountable to the MD/CEO for findings in non-compliance to this policy while educating contractors, vendors, employees on how to comply with this policy.
c. The Information Technology department being the electronic data custodian is responsible for specifying and implementing the information security controls for each level of data classification and implementing the technical controls which support the enforcement of this policy.
d. The data users are responsible for complying with the policy by adopting the administrative process and procedures which support this policy.

DATA CLASSIFICATION LEVELS

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to BEDC should that data be disclosed, altered, or destroyed without authorization. Data classification reflects the level of impact to BEDC if confidentiality, integrity, or availability of the data are compromised. The classification of data also helps determine what security controls are appropriate. All BEDC data are classified into one of four levels, or classifications as follows:

Confidential

Confidential information is information that, if made available to unauthorized parties, may adversely affect the business of BEDC. This classification also includes data that BEDC is required to keep confidential, either by law (e.g., NITDA) or under a confidentiality agreement with a third party, such as a vendor. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported. **Confidential information is strictly**

for the use of the recipient of the information and is not to be re-circulated to any unauthorized party.

Any unauthorized disclosure or loss of confidential data must be reported to the Internal Audit Department and Information Technology Incident Response Team. Examples of Confidential information include:

• Information covered by the National Information Technology Development Agency (NITDA), which requires protection of customer records. This includes pictures of customers kept for official purposes.

• Personally, Identifiable Information (PII) entrusted to BEDC care that is not otherwise categorized as Restricted Use data, such as information regarding application for supply, and information covered by the National Information Technology Development Agency (NITDA).

• BEDC staff ID Number, when stored with other identifiable information such as name or e-mail address, Individual employment information, including salary benefits, and performance appraisals.

• Legally privileged information.

• Information that is the subject of a confidentiality agreement.

• Other information/documents as deemed confidential based on Management's discretion.

Restricted Use

Restricted Use data includes any information that BEDC has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. In some cases, unauthorized disclosure or loss of this data would require BEDC to notify the affected individual and state or federal authorities. In some cases, modification of the data would require informing the affected individual.

BEDC's obligations will depend on the particular data and the relevant contract or laws. The minimum-security standards set a baseline for all Restricted Use data. Systems and processes protecting the following types of data need to meet that baseline:

• Personally, identifiable health information that is not subject to NITDA but included in the staff file.

• Unencrypted data used to authenticate or authorize individuals to use electronic resources, such as passwords, keys, and other electronic tokens.

• “Criminal Background Data" that might be collected as part of an application form or a background check.

More stringent requirements exist for some types of Restricted Use data. Staff working with the following types of data must follow BEDC policies governing those types of data and consult with the Information Technology department to ensure they meet all the requirements of their data type:

• Protected Health Information (PHI).

• Financial account numbers covered by the Payment Card Industry Data Security Standard (PCI-DSS), which controls how credit card information is accepted, used, and stored.

• Nigerian Government Classified Data.

Restricted Use data should be used only when no alternative exists and must be carefully protected. Any unauthorized disclosure, unauthorized modification, or loss of restricted use data must be reported to the Internal Audit Department and Information Technology Incident Response Team.

Internal

Internal data is information that is potentially sensitive and is not intended to be shared with the public. Internal data generally should not be disclosed outside of BEDC without the permission of the department that created the data. It is the responsibility of the data owner to designate information as 'Internal' where appropriate.

Examples of Internal data include: Some memos, correspondence, and minutes of meetings, contact lists that contain information that is not publicly available; and procedural documentation that should remain private.

Public

Public data is information that may be disclosed to any person regardless of their affiliation with BEDC. The public classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that do not require any level of protection from disclosure. While it may be necessary to protect original (source) documents from unauthorized modification, public data may be shared with a broad audience both within and outside the BEDC community and no steps need be taken to prevent its distribution.

Examples of public data include press releases, directory information, empty contractor forms, and other general information that is openly shared. The type of information BEDC posts on its website is a good example of public data.

PROCEDURES

Access to Confidential, Restricted and/or Internal data must be controlled from creation to destruction. Access to Confidential, Restricted and/or Internal data must be requested for an individual by their supervisor and then authorized by the data owner. Access to Confidential, Restricted and/or Internal data may be authorized to groups of persons by their job classification or responsibilities ("role-based" access) and may also be limited by a staff's department.

DATA COLLECTIONS

Data owners will assign a single classification to a collection of BEDC information; in other words, a data collection, which is common in purpose or function. When classifying a data collection, the most restrictive classification of any of the individual data elements should be used. For example, if data collection consists of Personally Identifiable Information (PII) entrusted to BEDC, the data collection must be classified as Confidential Data because one data element is considered Confidential.

DATA HANDLING REQUIREMENTS

For each classification, several data handling requirements are defined to appropriately safeguard the information. It is important to understand that overall sensitivity of BEDC information encompasses not only its confidentiality but also the need for integrity and availability.

ENFORCEMENT

Any employee found to have violated this policy may be subjected to disciplinary action as determined by Management.